

AVG 8.0 Email Server Edition

User Manual

Document revision 80.9 (12.8.2008)

Copyright AVG Technologies CZ, s.r.o. All rights reserved.
All other trademarks are the property of their respective owners.

This product uses RSA Data Security, Inc. MD5 Message-Digest Algorithm, Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991.

This product uses code from C-SaCzech library, Copyright (c) 1996-2001 Jaromir Dolecek
<%dolecek@ics.muni.cz%>

This product uses compression library zlib, Copyright (c) 1995-2002 Jean-loup Gailly and Mark Adler.

Contents

1. Introduction	4
2. AVG Installation Requirements	5
2.1 Operation Systems Supported	5
2.2 Email Servers Supported	5
2.3 Minimum Hardware Requirements	6
2.4 Recommended Hardware Requirements	6
2.5 Uninstall Previous Versions	6
2.6 Install AVG Fileserver	7
2.7 AVG Installation Options	7
3. AVG For MS Exchange Server	8
3.1 Specific Installation Requirements	8
3.1.1 MS Exchange Service Packs	8
3.2 Installation	8
3.2.1 Installation Launch	8
3.2.2 License Agreement	8
3.2.3 Registration	8
3.2.4 Location	8
3.2.5 Start Copying Files	8
3.2.6 Installation Finished	8
3.2.7 Restarting the Store Service	8
3.3 Configuration	12
3.3.1 Status	12
3.3.2 VSAPI 2.0	12
3.3.3 General Properties	12
3.3.4 Diagnostics Logging	12
3.4 Server Monitoring	16
3.4.1 Online Monitoring	16
3.4.2 Event Log	16
4. AVG for Lotus Notes/Domino Server	20
4.1 Installation	20
4.1.1 Installation Launch	20
4.1.2 License Agreement	20
4.1.3 Registration	20

4.1.4 Location	20
4.1.5 Notes Ini File	20
4.1.6 Installation Finished	20
4.1.7 Restarting The Mail Server	20
4.2 Program Launch	22
4.3 Configuration	24
4.3.1 Global Settings	24
4.3.2 Mail Scan	24
4.3.3 Scheduled Database Scan	24
4.4 AVG Virus Vault	29
4.5 AVG Log Files	31
5. E-mail Scanner	33
5.1 Certification	34
5.2 Mail Filtering	35
6. FAQ and Technical Support	36

1. Introduction

This user manual provides comprehensive documentation for **AVG 8.0 Email Server Edition**.

Congratulations on your purchase of AVG 8.0 Email Server Edition!

AVG 8.0 Email Server Edition is one of a range of award winning AVG products designed to provide you with peace of mind and total security for your PC. As with all AVG products **AVG 8.0 Email Server Edition** has been completely re-designed, from the ground up, to deliver AVG's renowned and accredited security protection in a new, more user friendly and efficient way.

AVG has been designed and developed to protect your computing and networking activity. Enjoy the experience of full protection from AVG.

2. AVG Installation Requirements

2.1. Operation Systems Supported

AVG 8.0 Email Server Edition is intended to protect e-mail servers running under the following operating systems:

- Windows 2008 x64 Server Edition
- Windows 2003 Server (x86, x64 and Itanium) SP1
- Windows 2000 Server SP4 + Update Rollup 1
- Windows 2000/XP, workstation edition (Kerio MailServer 5.0/6.0)

(and possibly higher service packs for specific email servers)

Note: AVG 8.0 File Server Edition *must be installed on your computer in order to ensure e-mail antivirus and antispymware protection using the AVG scanning engine!*

2.2. Email Servers Supported

There are several installations of **AVG 8.0 Email Server Edition** available. Each one covers specific email servers, as listed below:

- **AVG for MS Exchange 2000/2003 Server** – MS Exchange 2000 Server (with Service Pack 1 or higher), and MS Exchange 2003 Server versions.

Note: for Exchange 2000 Server - Service Pack 1 (or higher) needs to be applied before you can use the AVG engine; **AVG for MS Exchange 2000/2003 Server** uses the VSAPI 2.0 (or 2.5 with Exchange 2003 Server) application interface which is covered in this Service Pack.

- **AVG for MS Exchange 2007 Server** – MS Exchange 2007 Server version
- **AVG for Lotus Notes/Domino Server** – Lotus Notes/Domino Server version 5.0 and higher

2.3. Minimum Hardware Requirements

Minimum hardware requirements for **AVG 8.0 Email Server Edition** are as follows:

- Intel Pentium CPU 300 MHz
- 70 MB of free hard drive space (for installation purposes)
- 64 MB of RAM memory

2.4. Recommended Hardware Requirements

Recommended hardware requirements for **AVG 8.0 Email Server Edition** are as follows:

- Intel Pentium CPU 600 MHz
- 70 MB of free hard drive space
- 256 MB of RAM memory

2.5. Uninstall Previous Versions

If you have an older version of AVG Email Server installed, you will need to uninstall it manually before installing **AVG 8.0 Email Server Edition**. You must manually perform the uninstallation of the previous version, using the standard windows functionality.

- From the start menu **Start/Settings/Control Panel/Add or Remove Programs** select the correct program from the list of installed software. Be careful to select the correct AVG program for uninstallation. You need to uninstall the Email Server Edition before uninstalling the AVG File Server Edition.
- Once you have uninstalled the Email Server Edition, you can proceed to uninstall your previous version of AVG File Server Edition. This can be done easily from the start menu **Start/All Programs/AVG/Uninstall AVG**

When both the AVG Email Server and the AVG File Server have been successfully uninstalled - proceed with installation of the latest AVG 8.0 File Server Edition.

2.6. Install AVG Fileserver

AVG 8.0 File Server Edition is required to ensure e-mail antivirus and antispyware protection using the AVG scanning engine! It must be installed BEFORE beginning the installation of **AVG 8.0 Email Server Edition**. For details on **AVG 8.0 File Server Edition** installation, please refer to the **AVG 8.0 File Server Edition** User Manual document available from the [AVG website](http://www.avg.com) (www.avg.com) **Downloads** section.

2.7. AVG Installation Options

AVG can be installed either from the installation file available on your installation CD, or you can download the latest installation file from the [AVG website](http://www.avg.com) (www.avg.com).

Before you start installing AVG, we strongly recommend that you visit the AVG website to check for a new installation file. This way you can be sure to install the latest available version of AVG 8.0 Email Server Edition.

During the installation process you will be asked for your license/sales number. Please make sure you have it available before starting the installation. The sales number can be found on the CD packaging. If you purchased your copy of AVG on-line, your license number will have been delivered to you via e-mail.

For more information, navigate to the specific chapter according to your installed e-mail server.

- [AVG For MS Exchange Server](#) This chapter covers both **AVG for MS Exchange 2000/2003 Server** and **AVG for MS Exchange 2007 Server**. Though these editions have separate installation files, they function in effectively the same way (similar dialogs and configuration methods).
- [AVG for Lotus Notes/Domino Server](#)

3. AVG For MS Exchange Server

This chapter covers both **AVG for MS Exchange 2000/2003 Server** and **AVG for MS Exchange 2007 Server**. Though these editions have separate installation files, they function in effectively the same way (similar dialogs and configuration methods).

3.1. Specific Installation Requirements

3.1.1. MS Exchange Service Packs

Since **AVG for MS Exchange 2000/2003 Server** uses the VSAPI 2.0/2.5 virus scanning interface, you must have the Service Pack 1 (or higher) for MS Exchange 2000 Server applied on your system. Follow the link below to get the latest Service Pack for MS Exchange 2000 Server:

Service Pack for MS Exchange 2000 Server:

<http://www.microsoft.com/technet/prodtechnol/exchange/downloads/2000/sp3/default.msp>

For MS Exchange 2003 Server no additional service pack is needed; however, it is recommended to keep your system as up to date with the latest service packs and hotfixes as possible in order to obtain maximal available security.

Service Pack for MS Exchange 2003 Server (optional):

<http://www.microsoft.com/exchange/evaluation/sp2/overview.msp>

At the beginning of the setup, all system libraries versions will be examined. If it is necessary to install newer libraries, the installer will rename the old ones with a .delete extension. They will be deleted after the system restart.

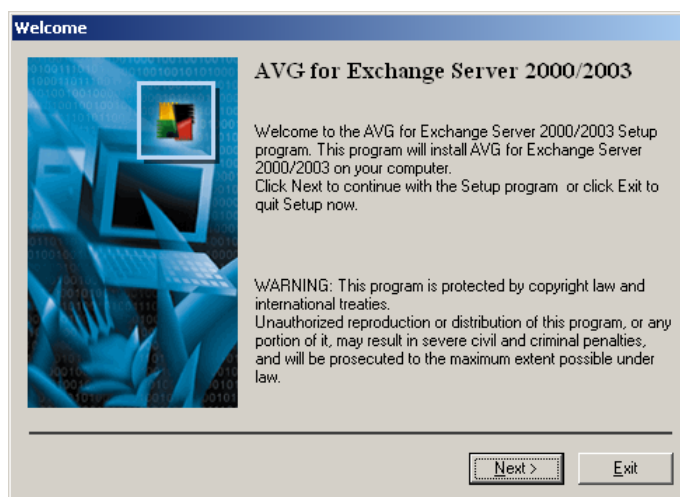
3.2. Installation

To install AVG on your computer, you need to get the latest installation file. You can use the installation file from the CD that is a part of your box edition but this file might be out-of-date. Therefore we recommended getting the latest installation file online. You can download the file from the [AVG website](http://www.avg.com) (at www.avg.com) / **Downloads** section.

Once you have downloaded and saved the installation file on your hard disk, you can launch the installation process. The installation is a sequence of dialog windows with a brief description of what do at each step. In the following, we offer an explanation

for each dialog window:

3.2.1. Installation Launch



The installation process starts with the **Welcome** window. Click on the **Next** button to continue to the next dialog.

3.2.2. License Agreement

This dialog provides the full wording of the AVG license agreement. Please read it carefully and confirm that you have read, understood and accept the agreement by pressing the **Accept** button. If you do not agree with the license agreement press the **Don't accept** button, and the installation process will be terminated immediately.

3.2.3. Registration

In this screen you should fill in your **AVG 8.0 Email Server Edition** license number.

If you used an **AVG 8.0 Email Server Edition** license number during the installation of **AVG 8.0 File Server Edition** then this screen will not be displayed. However if you purchased **AVG 8.0 Email Server Edition** and **AVG 8.0 File Server Edition** separately, then you will now need to enter your license number for **AVG 8.0 Email Server Edition**.

Confirm the provided information by clicking the **Next** button.

Having confirmed the license agreement you will be redirected to the **Checking**

System Status dialog. This dialog does not require any intervention; your system is being checked before the AVG installation can start. Please wait until the process has finished, then continue automatically to the following dialog.

3.2.4. Location

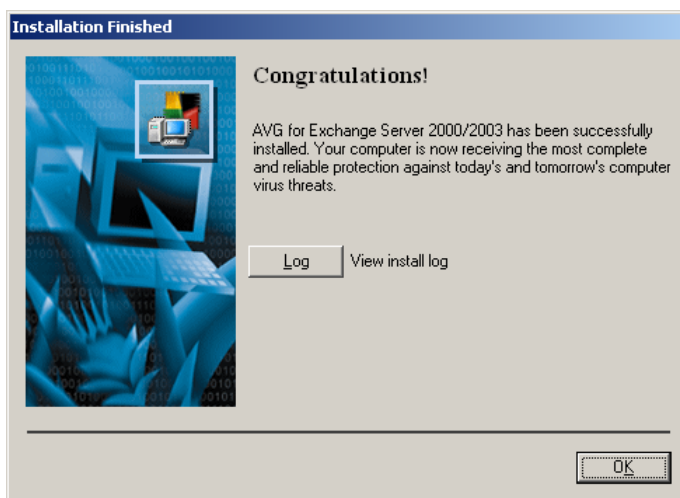
In the next window you will be prompted to select the target installation folder. Press the Browse button to select other location than the default one. If you do not have an actual reason to change the default settings, it is recommended to keep the preset location. Click on the Next button to continue.

3.2.5. Start Copying Files

Setup prompts you to trigger copying of the installation files before the installation will be completed. Accept it by clicking on the Next button.

3.2.6. Installation Finished

Once the installation wizard has copied all necessary files to your hard drive, the installation will be completed.



You can view the installation log file by pressing the Log button:

```

setup.log - Notepad
File Edit Format View Help
---
Installing AVG for Exchange Server 2000 at Wed Oct 11 15:27:09 2006
Closing setup library ... done
---
Installing AVG for Exchange Server at Wed Oct 11 15:29:16 2006
Closing setup library ... done
---
Installing AVG for Exchange Server 2000 at Tue Oct 17 12:40:44 2006
STORE.EXE version = 6.5.6944.3
Installation directory: C:\AVG4ES2K
Installation phase: 0
Copying file setupes.exe to C:\AVG4ES2K\setupes.exe
Copying file setupes.dll to C:\AVG4ES2K\setupes.dll
Copying file setupes.lng to C:\AVG4ES2K\setupes.lng
Copying file setwzes.dll to C:\AVG4ES2K\setwzes.dll
Copying file avg4es2k.dll to C:\AVG4ES2K\avg4es2k.dll
Copying file avgintf.dll to C:\AVG4ES2K\avgintf.dll
Copying file avg4es2ksi.dll to C:\AVG4ES2K\avg4es2ksi.dll
Copying file avg4es2k.xml to C:\AVG4ES2K\dat\avg4es2k.xml
Copying file expat.dll to C:\WINDOWS\system32\expat.dll
Progress: Program registration
Progress: Restarting the Store service, please wait

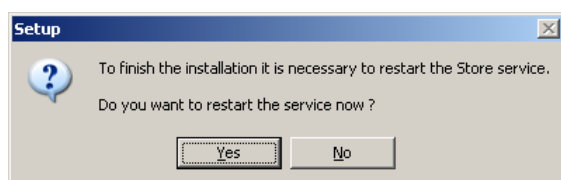
```

You can also view the setup log later as the setup.log file in your system temporary folder.

Press the **OK** button in the **Installation Finished** window to close the setup dialog.

3.2.7. Restarting the Store Service

During the installation process, or after closing the setup dialog, you will be prompted to restart the Exchange 2000/2003 Server Store service:



Press the **Yes** button to restart the Store service with all **AVG for MS Exchange 2000/2003** components included. Then you can start to use the product.

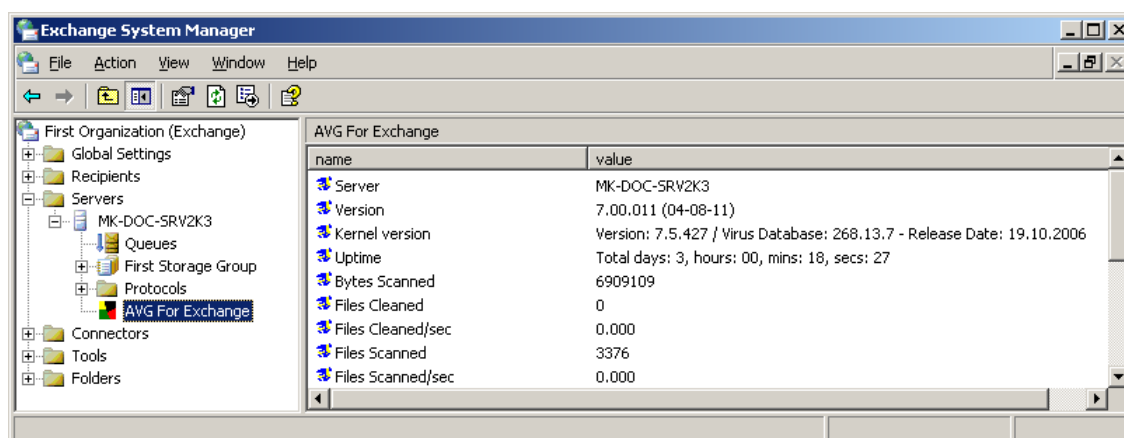
Note: Restarting the service will make your server unreachable for some time! You should warn your users before restarting the service because all users online will be automatically disconnected during the restart.

3.3. Configuration

When the Exchange 2000/2003 Server Store service is restarted after **AVG for MS Exchange 2000/2003 Server** has been installed, no further actions are needed to be taken to launch it.

3.3.1. Status

To view the status of **AVG**, launch the MS Exchange System Manager application. In the Servers branch of the control tree (*on the left side of the main window*) select the particular server. There is the AVG for Exchange branch in the server's sub-tree. Selecting this branch will open the information window showing various data to be overviewed.



The information displayed in the window include server name, application version, database version, kernel version, and the total time of program run since the last restart. Also, items informing about anti-virus performance are displayed here (*performance monitor counters*).

AVG for MS Exchange 2000/2003 Server scans all messages in the databases of private and public folders. If a virus is found, AVG for MS Exchange 2000/2003 Server writes a message into the AVG log file and also into the Event Log.

3.3.2. VSAPI 2.0

Virus Scanning **API 2.0** (VSAPI 2.0 as provided in MS Exchange 2000 Server) does not allow the deletion of infected e-mail files. Since the virus infected e-mail message attachment cannot be deleted, its filename is changed: AVG for Exchange 2000/2003 Server appends the .virusinfo.txt extension to the original filename. The file content is overwritten with a message about the known virus. If a virus is found directly in the

message, the whole body of the message is overwritten with a note saying a virus was found inside this message.

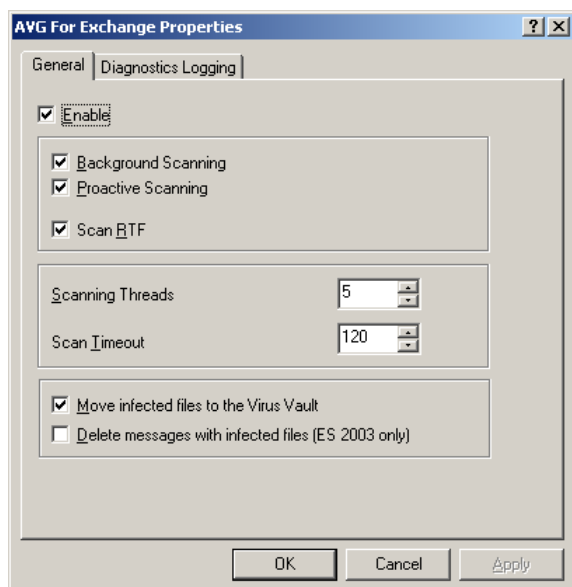
Virus Scanning **API 2.5** (*VSAPI 2.5 as provided in MS Exchange 2003 Server*) also allows deletion of infected messages. This feature can be set up in AVG for MS Exchange 2000/2003 Server configuration dialog.

3.3.3. General Properties

The AVG for Exchange 2000/2003 Server configuration window can be opened by right clicking on the **AVG for Exchange** branch, and selecting the **Properties** item. Alternatively, you can open the window using the **Action** button from the upper menu.

The **AVG for Exchange Properties** configuration window consists of two tabs. You can change the e-mail virus scanning settings and the logging behavior here.

General Tab



On the **General** tab you will find several preset options related to the AVG for MS Exchange 2000/2003 Server e-mail virus scanning performance:

- **Enable** – you can enable or disable mail scanning here.
- **Background Scanning** – you can enable or disable the background scanning process here. Background scanning is one of the features of the VSAPI 2.0/2.5 application interface. It provides threaded scanning of the Exchange Messaging

Databases. Whenever an item that has not been scanned before is encountered in the users' mailbox folders, it is submitted to AVG for Exchange 2000/2003 Server to be scanned. Scanning and searching for the not examined objects runs in parallel.

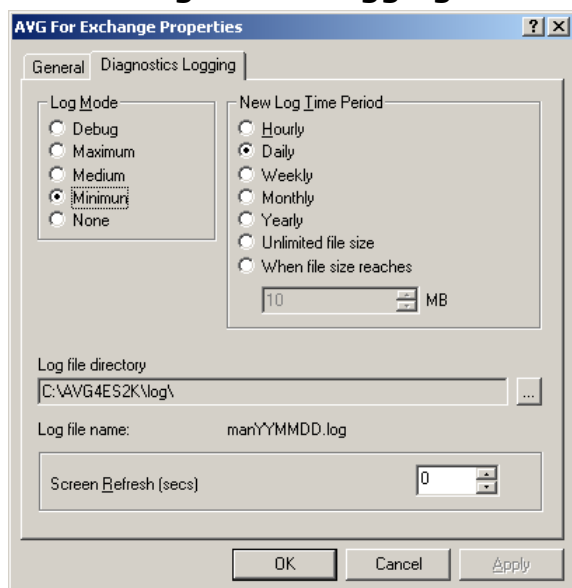
- A specific low priority thread is used for each database, which guarantees other tasks (e.g. e-mail messages storage in the Microsoft Exchange database) are always carried out preferentially.
- **Proactive Scanning** – you can enable or disable the proactive scanning function of VSAPI 2.0/2.5 here. The proactive scanning lies in dynamical priority management of items in scanning queue. The lower priority items are not being scanned unless all the higher priority ones (most frequently supplied on demand in the queue) have been scanned. However, an item's priority rises if a client tries to use it, so the items' precedence changes according to users' activity.
- **Scan RTF** – you can specify here, whether the RTF file type should be scanned or not.
- **Scanning Threads** – the scanning process is threaded by default to increase the overall scanning performance by a certain level of parallelism. You can change the threads count here. The default number of threads is computed as 2 times the 'number_of_processors' + 1.
- **Scan Timeout** field – the maximum continuous interval (in seconds) for one thread to access the message that is being scanned.
- **Move infected files to the Virus Vault** – if checked on, every infected e-mail message file will be moved into **AVG Virus Vault** quarantine environment.
- **Delete messages with infected files (ES 2003 only)** – after checking this item on, a message where a virus is detected will be deleted. When this item is checked off, the infected e-mail is delivered to recipient, but infected attachment is replaced with a text file containing information on the virus detected. This option is available only in VSAPI 2.5 in Exchange 2003 Server.

Generally, all the features on this tab are user extensions of the Microsoft VSAPI 2.0/2.5 application interface services. For the detailed information on the VSAPI 2.0/2.5 please refer to the following links (and also the links accessible from the referenced ones):

- <http://support.microsoft.com:80/support/kb/articles/Q285/6/67.ASP> for general info on the VSAPI 2.0 in Exchange 2000 Server Service Pack 1
- <http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k> for information on Exchange and antivirus software interaction
- <http://support.microsoft.com/default.aspx?scid=kb;en-us;823166> for information on additional VSAPI 2.5 features in Exchange 2003 Server application.

Note: The scanning behavior is controlled from the AVG File Server Application. From the application's main menu select Tools/Advanced Settings. (See the [E-mail Scanner](#) chapter).

3.3.4. Diagnostics Logging



On this tab you can define the virus scanning logging frequency and general behavior here. Several fields are preset on the Diagnostics Logging tab:

- **Log Mode** – you can adjust the amount of information to be logged here.
- **New Log Time Period** – you can define the period of new log file creation, and possibly the log file size here.
- **Log file directory** – you can change the default log file location here.
- **Log file name** – you can see the default log filename here.
- **Screen Refresh (secs)** – you can specify how often the online monitoring screen (shown on the AVG for Exchange 2000/2003 Server information window) should be refreshed.

3.4. Server Monitoring

3.4.1. Online Monitoring

Server	MK-DOC-SRV2K3
Version	7.00.011 (04-08-11)
Kernel version	Version: 7.5.427 / Virus Database: 268.13.7 - Release Date: 19.10.2006
Uptime	Total days: 3, hours: 01, mins: 02, secs: 02
Bytes Scanned	6909109
Files Cleaned	0
Files Cleaned/sec	0.000
Files Scanned	3376
Files Scanned/sec	0.000
Folders Scanned in Background	66
Messages Cleaned	0
Messages Cleaned/sec	0.000
Messages Scanned in Background	2440
Messages Processed	2452
Messages Processed/sec	0.000
Messages Deleted	0
Messages Deleted/sec	0.000
Queue Length	0
Waiting files	0

In the AVG for MS Exchange 2000/2003 Server information window (*Refer to the [beginning](#) of this section to see how to get there.*), there are several fields displayed:

The first four items provide general information on the server and AVG for Exchange 2000/2003 Server status:

- **Server** – server name
- **Version** – version of AVG for Exchange 2000/2003 Server
- **Kernel version** – version of the Anti-Virus kernel, and its internal virus database
- **Uptime** –total time since the last Exchange 5.x Server restart

The other items represent particular VSAPI 2.0/2.5 performance monitor counters related to virus scanning of Exchange 2000/2003 Server. Counters are described as follows:

- **Bytes Scanned** – total number of bytes in all files processed by the virus scanner
- **Files Cleaned** – total number of separate files cleaned by the virus scanner

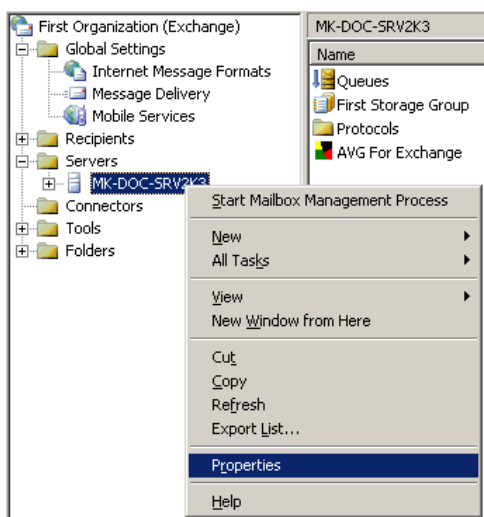
- **Files Cleaned/sec** – rate at which separate files are cleaned by the virus scanner
- **Files Quarantined** – total number of separate files moved to quarantine by the virus scanner
- **Files Quarantined/sec** – rate at which separate files are put into quarantine by the virus scanner
- **Folders Scanned in Background** – total number of folders processed by background scanning
- **Messages Cleaned** – total number of top-level messages cleaned by the virus scanner
- **Messages Cleaned/sec** – rate at which top-level messages are cleaned by the virus scanner
- **Messages Quarantined** – total number of top-level messages moved to quarantine by the virus scanner
- **Messages Quarantined/sec** – rate at which top-level messages are put into quarantine by the virus scanner
- **Messages Processed** – cumulative value of the total number of top-level messages processed by the virus scanner
- **Messages Processed/sec** – rate at which top-level messages are processed by the virus scanner
- **Messages Scanned in Background** – total number of messages processed by background scanning
- **Messages Deleted** – total number of suspect messages deleted by virus scanner (available only in VSAPI 2.5)
- **Messages Deleted/sec** – rate at which suspect messages are deleted by virus scanner (available only in VSAPI 2.5)
- **Queue Length** – current number of outstanding requests that are queued for virus scanning
- **Waiting Files** – count of files waiting to be scanned

3.4.2. Event Log

Except for the online monitoring of AVG for MS Exchange 2000/2003 Server you can also setup the virus scanner related events logging within the **Event Log**. Available events cover many issues, such as program libraries loading notes, virus-found events, troubleshooting warnings, etc.

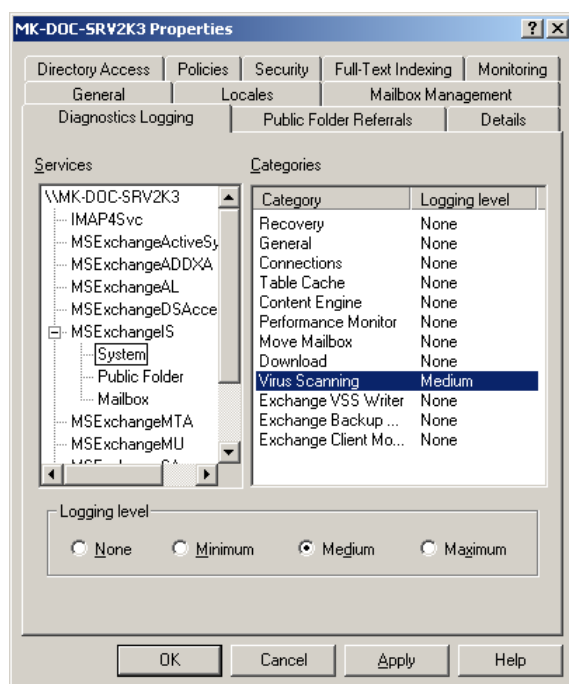
You can set up the logging level of Exchange VSAPI 2.0/2.5 in the Exchange System Manager's main window (*as shown in the [beginning](#) of this section*).

- Double-click the **Servers** branch in the control tree
- Select the particular server (see an example server name highlighted in the picture below)
- Right-click the server name, and select the **Properties** item from the context menu



- The **Properties** window appears.
- Switch to the **Diagnostics Logging** tab
- From the **Services** tree select the MExchangeIS / System folder
- From the opened **Categories** list select the **Virus Scanning** item, and choose the desired logging level for the operating system Event Log component. The following levels are offered:

- None
- Minimum
- Medium
- Maximum



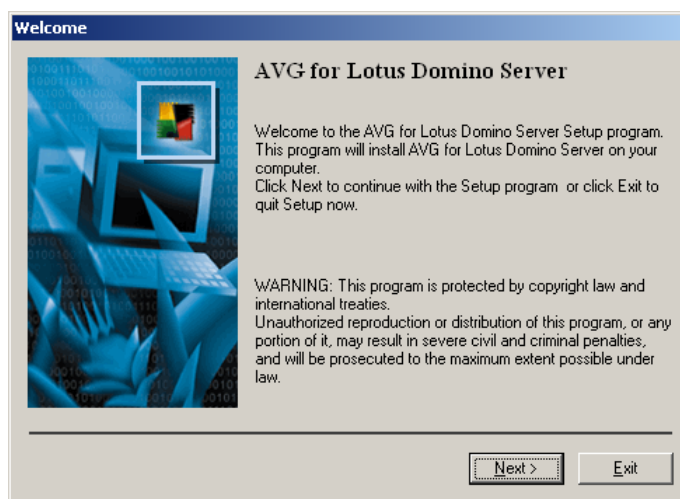
Note: You will find the complete description of the VSAPI 2.0/2.5 events on this link:
<http://support.microsoft.com/default.aspx?scid=kb;EN-US;294336>.

4. AVG for Lotus Notes/Domino Server

4.1. Installation

4.1.1. Installation Launch

Execute the installation package; the introduction screen will appear. Press the **Next** button to continue with the installation.



4.1.2. License Agreement

The next window provides the full wording of the **License Agreement**. Please read it carefully, and if you accept all the points, confirm your approval by clicking the **Accept** button.

4.1.3. Registration

In this screen you should fill in your **AVG 8.0 Email Server Edition** license number.

If you used an **AVG 8.0 Email Server Edition** license number during the installation of **AVG 8.0 File Server Edition** then this screen will not be displayed. However if you purchased **AVG 8.0 Email Server Edition** and **AVG 8.0 File Server Edition** separately, then you will now need to enter your license number for **AVG 8.0 Email Server Edition**.

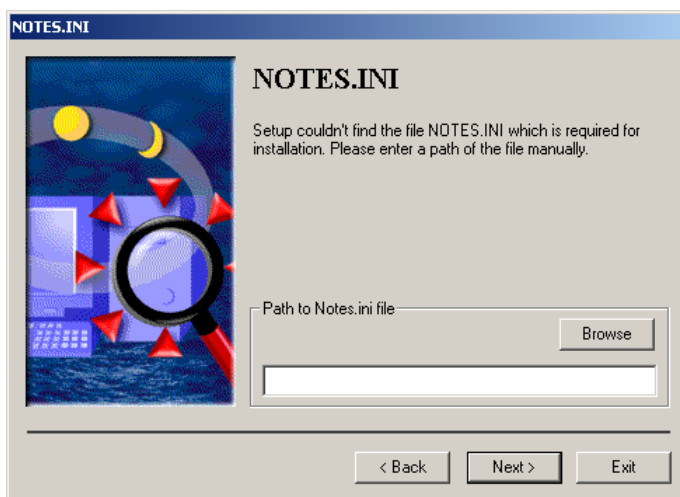
Confirm the provided information by clicking the **Next** button.

4.1.4. Location

Once you have agreed to the license agreement, you will be prompted to select the target installation folder. The **AVG for Lotus Notes/Domino Server** data and program files will be installed directly into the Lotus Notes/Domino folder. Press the Browse button to select a location other than the default one, though it is recommended to keep the default location. Click on the **Next** button to continue.

4.1.5. Notes Ini File

In order to install **AVG for Lotus Notes/Domino Server** correctly it is necessary to locate the Lotus Notes/Domino server configuration file NOTES.INI. If NOTES.INI is not found automatically, you will be prompted to set its path manually (by pressing the Browse button or by filling in the complete path directly). Click on the **Next** button to continue.



4.1.6. Installation Finished

Once the installation wizard has copied all of the necessary files to your hard drive, the installation is completed.

4.1.7. Restarting The Mail Server

In order to complete the installation, the Lotus Notes/Domino server must be restarted. This will automatically launch AVG for Lotus Notes/Domino Server (server services AvgScan and AvgMail) and create the AVG databases (Configuration, Log and Vault). All of these can be blocked in the appropriate configuration sections later if

needed.

Your computer is now receiving the most complete and reliable protection against computer virus threats.

The following files were installed:

- Lotus Notes/Domino program directory:
 - navgscan.exe – server application for checking databases
 - navgmail.exe – server anti-virus mail checking application
 - navghook.dll – library for holding mail in the MAIL.BOX database until it has been scanned for viruses
- Lotus Notes/Domino data directory:
 - avgsetup.ntf – configuration database template
 - avglog.ntf – log database template
 - avgvirus.ntf – virus vault template
 - avgsetup.nsf – configuration database
 - avglog.nsf – log database
 - avgvirus.nsf – virus vault database

4.2. Program Launch

AVG for Lotus Notes/Domino Server will be automatically launched when the Lotus Notes/Domino server is restarted.

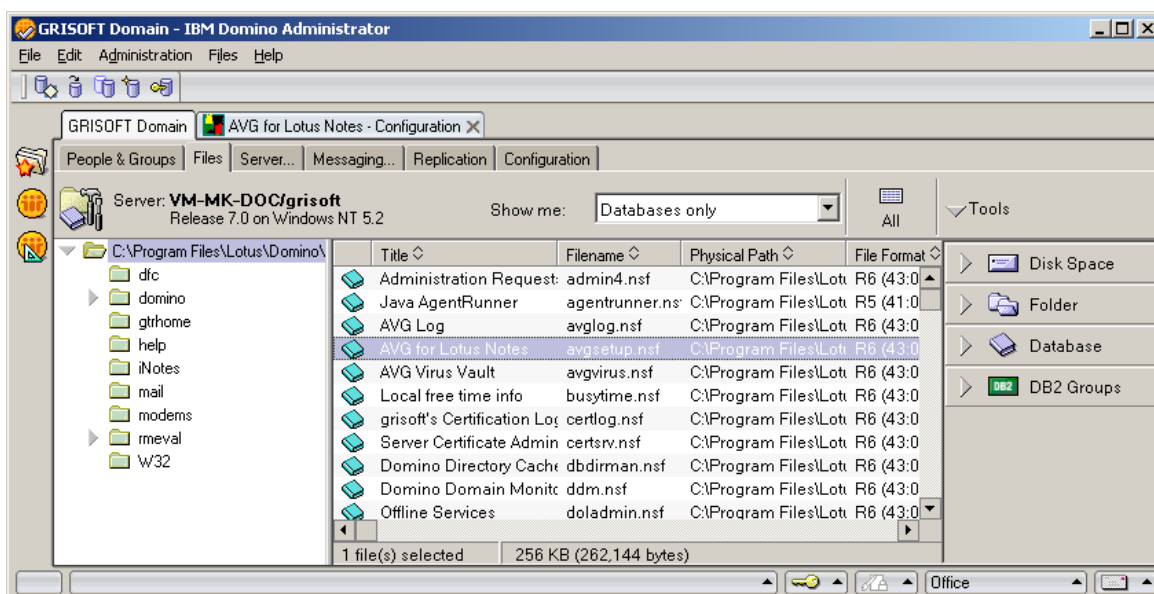
The default **AVG for Lotus Notes/Domino Server** settings for are as follows:

- scan all e-mails with attachments
- a certification message will be added to any e-mail which is virus-free, does not include a signature attachment, and has not been encrypted
- incoming files that are considered infected are sent to the recipient with a message containing file and virus details

- outgoing e-mail containing infected attachments will be returned to the sender with information about the infected objects and corresponding viruses; the infected e-mail will not be delivered to the recipient.

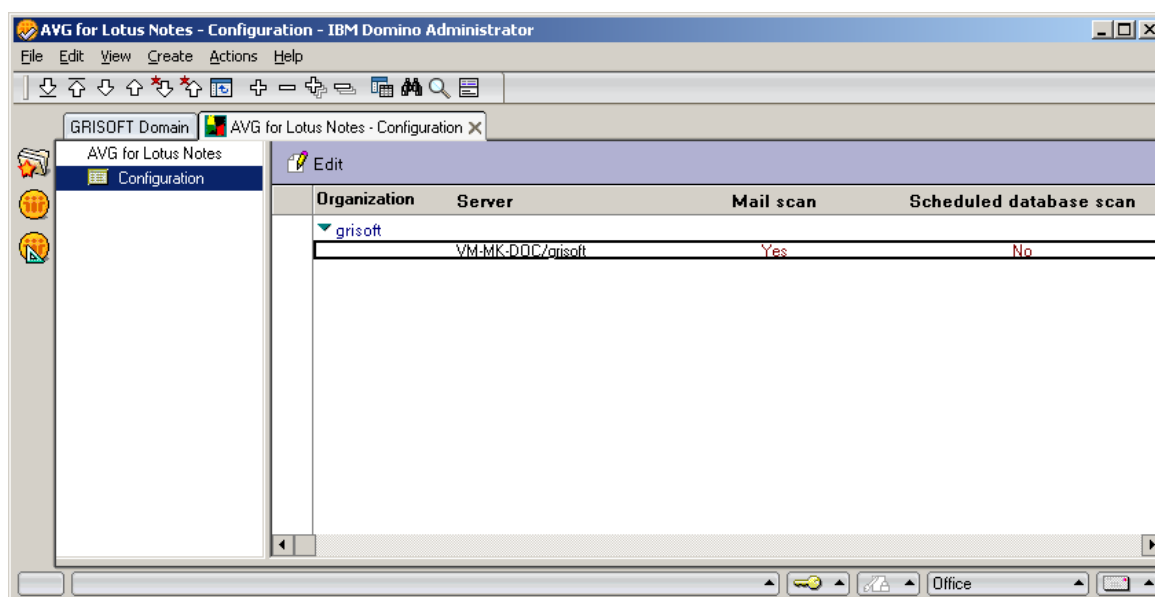
You can easily change the default configuration of **AVG for Lotus Notes/Domino Server** using the Domino Administrator utility. After selecting the **Files** tab in the initial window, you will see three AVG related files (Lotus databases literally) among all the files to administer:

- **AVG Log** (see section [AVG Log File](#))
- **AVG for Lotus Notes** (see section [Program Launch](#))
- **AVG Virus Vault** (see section [AVG Virus Vault](#))

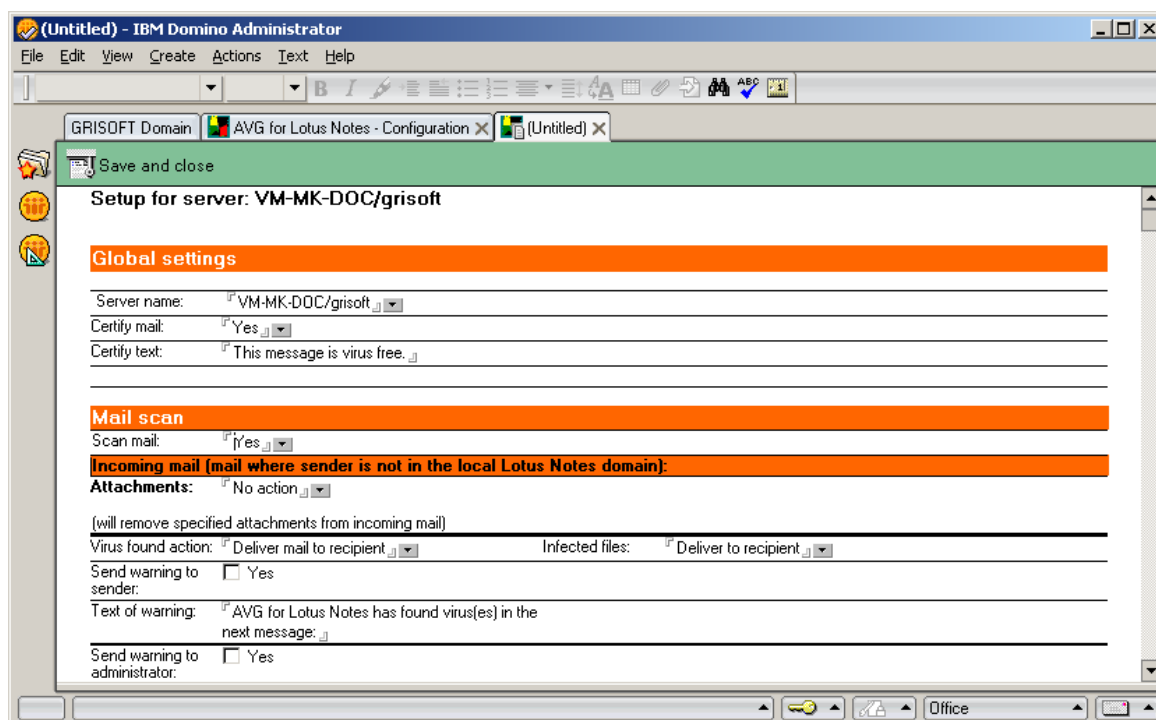


4.3. Configuration

Double click the **AVG for Lotus Notes** in the administrator utility main window / **File** tab to open the **AVG for Lotus Notes – Configuration** window.



In this window, select the server, on which you want to have the AVG configuration database. Double click on the server field, or simply press the Edit button that is right above the servers list. A new untitled window opens then within the Lotus administrator utility environment.



You can fully control the scanning and infected e-mail management behavior of AVG for Lotus Notes/Domino Server. Also you can schedule multiple Lotus database scans. To save the performed configuration changes, press the Save and close button in the upper area of the window.

All the configuration options fully corresponding to the fields presented on the screenshots above are as follows:

- [Global Settings](#) - Here you can specify server details
- [Mail Scan](#) - Here you can specify incoming/outgoing mail settings
- [Scheduled Database Scan](#) - Here you can specify the frequency and depth of database scanning

4.3.1. Global Settings

- **Server name** – the current server specification
- **Certify mail** – select whether AVG for Lotus Notes/Domino should certify e-mails or not

- **Certify text** – edit the certification text (e. g. "The message is virus-free...")

4.3.2. Mail Scan

- **Scan mail** – enable/disable the automatic e-mail anti-virus scan
- **Incoming Mail** (a mail, where sender is not in the local Lotus Notes domain)
 - **Attachments** – the option enables defining file extensions of e-mail attachments that should be automatically removed from the e-mail. Attachments with user-defined extensions will be automatically removed from an incoming e-mail message, no matter whether the identified file has been infected by a virus or not. The possible actions are:
 - **No action** - incoming attachments will not be filtered or removed
 - **Remove** - user defined attachments will be removed from virus-detected e-mail message, and then deleted
 - **Remove and store in the vault** - user defined attachments will be deleted from virus-detected e-mail, and moved to the Virus Vault

You will be allowed to choose the attachment file extensions from the list of keywords (or you can type a new one if the desired extension is not in the list) in a new Extensions field when the Remove or Remove and store... actions are selected.

Additionally, you can type in a customized text that will be inserted to the e-mail message body when the desired action was processed. Fill in an optional text to the Info text in mail field.

- **Virus found action** – you can specify action to be taken if a virus is found in an incoming e-mail:
 - **Deliver mail to the recipient** - the infected e-mail will be delivered to the recipient with a warning about the virus and infected file added.
 - **Return mail to sender** - the infected e-mail will be returned to the sender as undeliverable with an option to add a warning about the virus found.
 - **Infected files** - additional settings will define whether the infected attachments are removed from the email message and/or moved to the AVG Virus Vault. The Infected files field allows you to specify the

action to be taken for virus infected files. Possible actions are:

Remove – the infected files are removed from the e-mail

Remove and store in the vault – the infected files are removed from the e-mail and stored in the local Virus Vault

Store in the vault and deliver to recipient – the infected files are kept in the e-mail, and their copies are also stored in the local Virus Vault

Deliver to recipient – the infected files will be kept in the e-mail, and delivered to recipient

- **Send warning to recipient/sender** – you should select this field if you wish to warn the recipient/sender (depending on whether you choose Deliver mail to the recipient or Return mail to the sender action) of virus-infected e-mail.
- **Text of warning** – here you can edit the default message text included in the virus-infected email (if you have previously selected the Send warning to recipient/sender option).
- **Send warning to administrator** – when this field is selected, a warning will be sent to administrators specified in the Administrators field after an incoming e-mail is detected as virus-infected. You can edit the text of the warning message in the corresponding Text of warning field.

- **Outgoing Mail Settings**

- **Virus found action** – you can specify what action is to be taken if a virus is found in an outgoing e-mail message:
 - **Deliver mail to the recipient** - the infected e-mail message will be delivered to the recipient with a warning about the virus and infected file added.
 - **Return mail to sender** - the infected e-mail message will be returned to the sender as undeliverable with an option of adding a warning about the virus found
 - **Infected files** - additional settings will define whether the infected attachments are removed from the email message and/or moved to the AVG Virus Vault. The Infected files field allows you to specify the

action to be taken for virus-infected files. Possible actions are:

Remove – the infected files are removed from the e-mail

Remove and store in the vault – the infected files are removed from the e-mail and stored in local Virus Vault

Store in the vault and deliver to recipient – the infected files are kept in the e-mail, and copies are also stored in local Virus Vault

Deliver to recipient – the infected files will be kept in the e-mail, and delivered to recipient

- **Send warning to recipient/sender** – select this field if you wish to warn the recipient/sender (depending on whether you choose Deliver mail to the recipient or Return mail to the sender action) of virus-infected e-mail.
- **Text of warning** – here you can edit the default message text included in the virus-infected email message if you have previously selected the Send warning to recipient/sender option.
- **Send warning to administrator** – with this field selected, a warning will be sent to administrators specified in the Administrators field after an outgoing e-mail is detected as virus-infected. You can edit the text of the warning message in the corresponding Text of warning field.

4.3.3. Scheduled Database Scan

Scheduled database scan:	
Scan at times:	Scan <input type="checkbox"/> All attachments
Repeat interval of:	<input type="checkbox"/> minutes
Days of week:	Infected files: <input type="checkbox"/> Leave in the document
Scan:	<input type="checkbox"/> All databases
List of databases (files to scan):	
Send warning to administrator:	<input type="checkbox"/> Yes

You can plan the scanning of server databases in this area of the AVG for Lotus Notes/Domino Server configuration form. Various fields are available:

- **Scan at times** – specify a time interval and/or exact time to tell AVG for Lotus Notes/Domino Server when it should run the databases scanning
- **Repeat interval of** – specify a time period (in minutes) defining the

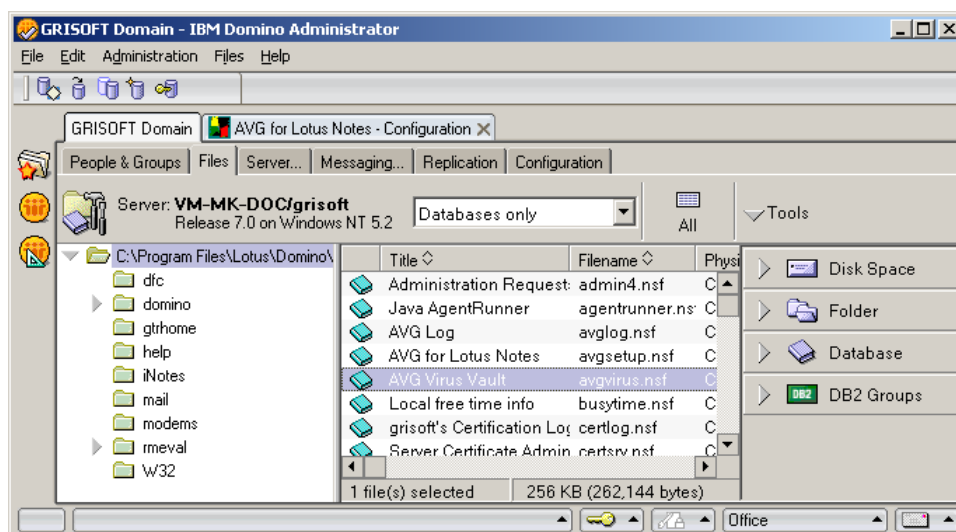
frequency of scans during the intervals specified in the Scan at times field

- **Days of the week** – you can select the days when database tests are run
- **Scan** (the attachments related field) – here you can define whether to check all the attachments or only those with extensions specified in the Extensions field
- **Infected files** - here you can specify the action to be taken for virus-infected files. Possible actions are:
 - **Remove** – the infected files are removed from the document
 - **Remove and store in Virus Vault** – the infected files are removed from the document, and stored in the local Virus Vault
 - **Leave in the document** - the infected files are kept in the document
- **Scan** (the databases related field) – here you can define whether to scan all the server databases or only those specified in the List of databases (files to scan) field
- **Send warning to administrator** – with this field selected, a warning will be sent to administrators specified in the Administrators field after a virus is detected during the database scan. You can edit the text of the warning message in the corresponding Text of warning field. You can define the subject line of the message. In the message body, a list of infected files (with links) and found viruses will be included.

Note: The scanning engine performance and the attachment filter are controlled from AVG. Please remember that the plugin settings in general cannot be configured in AVG. Features like e-mail scanning enabling/disabling, and e-mail certification can be configured only via AVG for Lotus Notes/Domino Server databases.

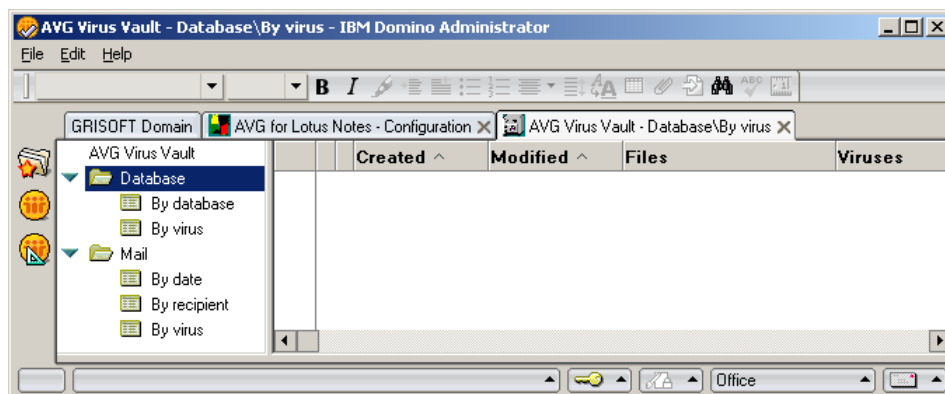
4.4. AVG Virus Vault

AVG for Lotus Notes/Domino Server Virus Vault is special server database where you can place the virus-infected files for safe further treatment (deletion or recovery) without risk of affecting the rest of your system resources.



In the Lotus Notes/Domino Server administration environment you can access the Virus Vault via the **AVG Virus Vault** database. Note that this database has nothing to do with the AVG Virus Vault application! It is a special Lotus Notes/Domino Server database. Double click the corresponding field in the Lotus administrator utility main window / **Files** tab to open and a new window will be opened.

You can examine the viruses stored in the Virus Vault according the following grouping parameters:



- **Grouped by Databases** (virus infected database files detected during database scans)

Additional sorting is divided into two categories:

- By database
- By virus

In each category there are four fields present by default:

- **Created** – the database creation timestamp
- **Modified** – the database modification timestamp
- **Files** – the infected files
- **Viruses** – the viruses found identification

- **Grouped by Mail**

Additional sorting is divided into three categories:

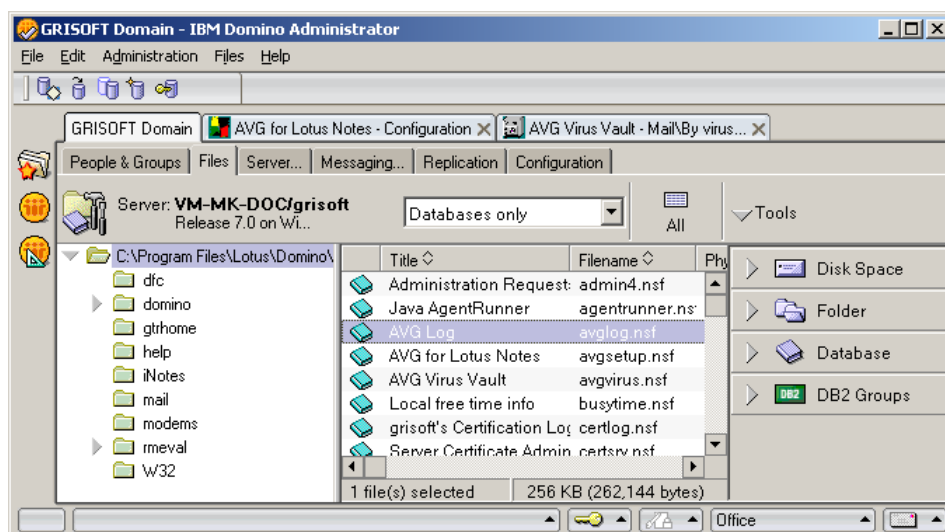
- By date
- By recipient
- By virus

In each category there are five fields present by default:

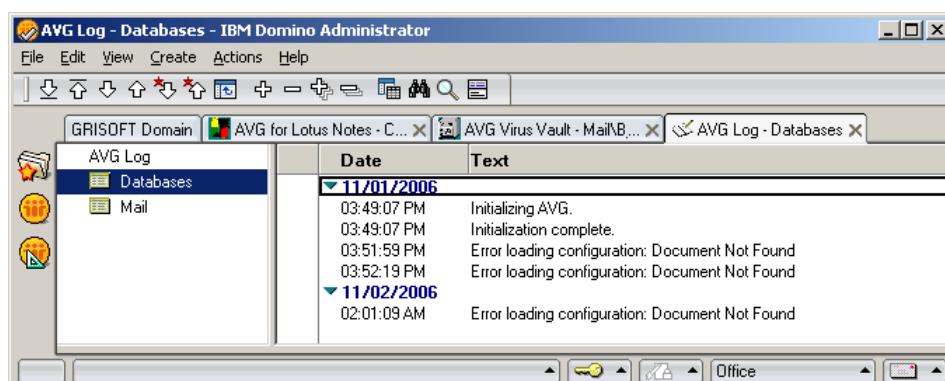
- **Time** – the infected e-mail delivery time
- **For** – the recipient info
- **From** – the sender info
- **Files** – the infected files identification
- **Viruses** – the viruses found identification

4.5. AVG Log Files

Information on **AVG for Lotus Notes/Domino Server** events recorded during the server's run is stored in the **AVG Log** file. Here you can review and further examine various events, such as initialization progress, viruses findings, etc.



In the Lotus Notes/Domino Server administration environment you can access the **AVG Log** file via the **AVG Log database**. Double click the corresponding field in the Lotus administrator utility main window/ **Files** tab to open new window.

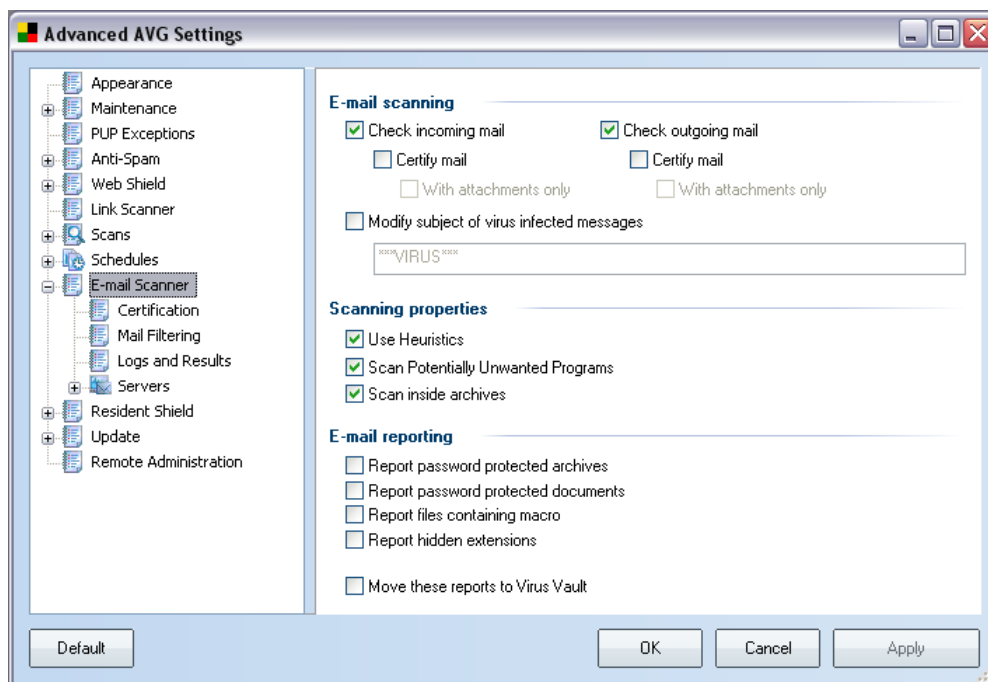


There are two fields present for both the **Databases** and **Mail** folders. Those are:

- **Date** – the timestamp of the logged record
- **Text** – the text of the log information

5. E-mail Scanner

The **E-mail Scanner** settings are configured from within the AVG File Server Edition. From the application's main menu select **Tools/Advanced Settings**. Then from the left menu in the **Advanced Settings** dialog, select the **E-Mail Scanner** item.

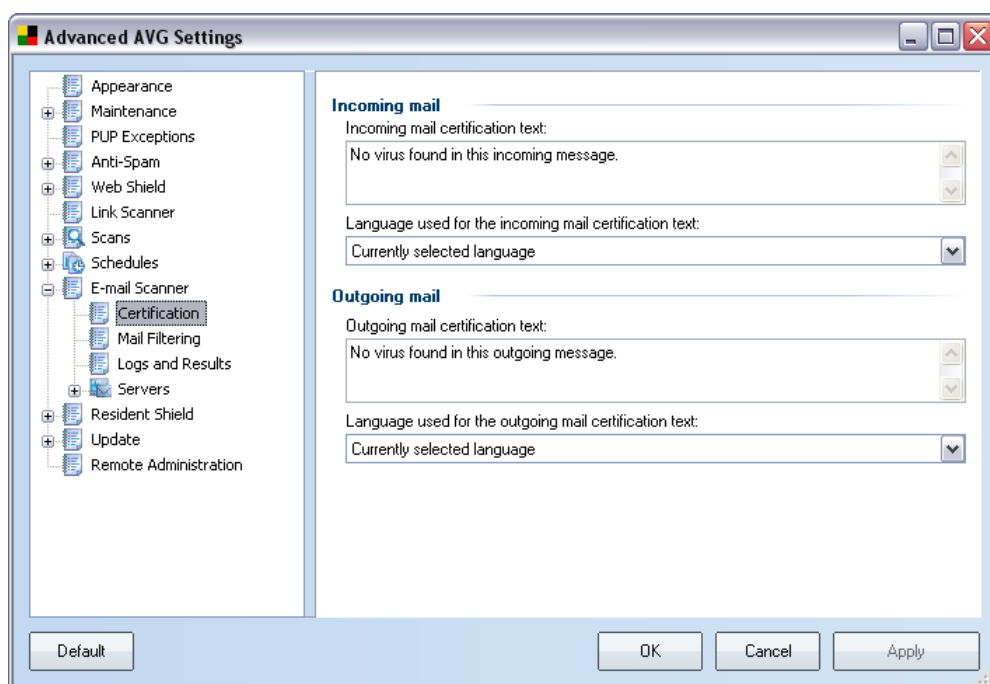


The **E-mail Scanner** dialog is divided into three sections:

- **E-mail scanning** - in this section select whether you want to scan the incoming/outgoing e-mail messages and whether all e-mails should be certified or only e-mails with attachments (*e-mail virus-free certification is not supported in HTML/RTF format*). Additionally you can choose if you want AVG to modify the subject for messages that contain potential viruses. Tick the **Modify subject of virus infected messages** checkbox and change the text respectively (*default value is ***VIRUS****).
- **Scanning properties** - specify whether the heuristic analysis method should be used during scanning (**Use heuristic**), whether you want to check for the presence of potentially unwanted programs (**Scan Potentially Unwanted Programs**), and whether archives should be scanned too (**Scan inside archives**).
- **E-mail reporting** - specify whether you wish to be notified via e-mail about

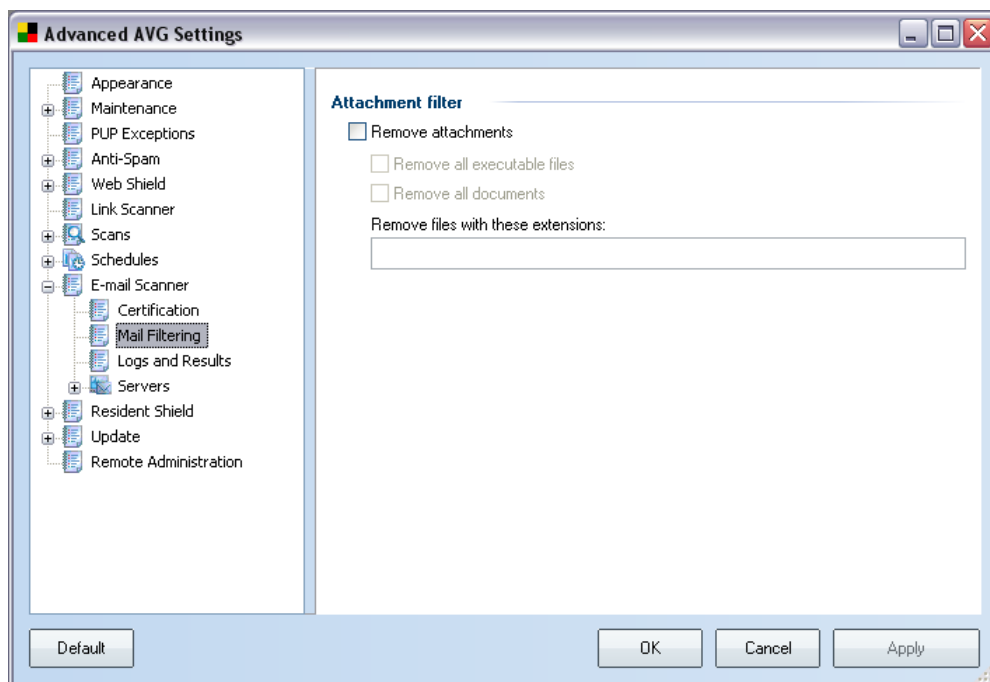
password protected archives, password protected documents, macro containing files and/or files with hidden extension detected as an attachment of the scanned e-mail message. If such a message is identified during scanning, define whether the detected infectious object should be moved to the **Virus Vault**.

5.1. Certification



In the **Certification** dialog you can specify exactly what text the certification note should contain, and in what language. This should be specified separately for **Incoming mail** and **Outgoing mail**.

5.2. Mail Filtering



The **Attachment filter** dialog allows you to set up parameters for e-mail messages attachment scanning. By default, the **Remove attachments** option is switched off. If you decide to activate it, all e-mail message attachments detected as infectious or potentially dangerous will be removed automatically. If you want to define specific types of attachments that should be removed, select the respective option:

- **Remove all executable files** - all *.exe files will be deleted
- **Remove all documents** - all *.doc files will be deleted
- **Remove files with these extensions** - will remove all files with the defined extensions

6. FAQ and Technical Support

Should you have any problems with your AVG, either business or technical, please refer to the **FAQ** section of the AVG website at www.avg.com.

If you do not succeed in finding help this way, contact the technical support department by email. Please use the contact form accessible from the system menu via **Help / Get help online**.